

REMARKS

Applicant encloses herewith a copy of sheet 4 of 9 of Saito, in which Applicant
5 has included comments regarding the disclosure of Saito and the features of the
present invention, as defined in the claims.

Throughout the claims, Applicant has replaced the term "start block" by the term
"header" as original supported by the fourth paragraph, second line of page 7 of
10 the translation of the PCT application as originally filed.

Applicant is of the opinion that the term "header" means exactly the same thing to
a person skilled in the art as the term "start block," so that the Examiner should
be able to accept this amendment after final without taking the position that the
15 Applicant has raised any new issues that would require an additional search.
Applicant requests that the Examiner give his opinion on that topic and on the
amended claims, without requiring Applicant to file a request for continued
examination (RCE).

20 Saito does not disclose a "start section" that remains unencrypted. The start
section of the user data block as outlined in the enclosed commented sheet 4 is
encrypted, because the start section is, as defined in the third paragraph and in
the fourth paragraph of Claim 1, the section of the user data block which follows
the header or start block. Thus, Saito definitely discloses to encrypt the first
25 section of the user data block, which follows the header, while the present
invention does not encrypt that section but only encrypts the second part.

The Examiner outlines on page 2 of the Office Action that he means with the
"start block" the left most unencrypted data block, which Applicant has indicated
30 as "second part" in Fig. 4G of Saito (attached).

This interpretation is, however, not justified, because the encrypted data portion to the left of the unencrypted data portion, which Applicant has indicated by a start section that also belongs to the “user data block” of Saito.

5 Furthermore, to make this even clearer, Applicant has replaced the term “start block” by the term “header” in the claims. The first encrypted data portion of Fig. 4G of Saito does not belong to the header, although Saito clearly distinguishes between a header and data. The same difference is presented in the wording of Claim 1, which distinguishes between the header and the user data block. The
10 third paragraph of Claim 1 makes it clear that the start section, which is unencrypted, follows the header and is the first part of the user data.

In Saito, the left-most unencrypted data portion is the second part of the user data and does not follow the header, and is also not the start section of the user
15 data block. Instead, the unencrypted data portion in Saito is behind the start section of the user data block. The start section of the user data block in Saito is, as becomes clear from the commented Fig. 4G, encrypted.

Regarding Applicant's provides argument B, the Examiner is in error when
20 stating that support for argument B is not included in the claims. Instead, argument B is included in the playback Claims 6 and 13, while the first argument (argument A) is included in the generating claims 1 and 12.

Regarding the Examiner's remarks on page 3, second paragraph, the Examiner
25 did not reject the independent claims based on a combination of Saito and Downs or Saito and Rump.

Regarding the objection against the drawings, enclosed please find a
replacement Fig. 5, in which Applicant has introduced the “only” feature.

30

Regarding the Examiner's objection to the specification, the Examiner is in error when stating that the "only" feature is not supported by the description. Please refer to page 16, second paragraph, line 6 of the translation of the PCT application as originally filed:

5

"According to the present invention only the information of the start block 12 which is absolutely necessary for playing back the unencrypted start section of the user data block 14 (step 110) is initially processed in the playback device." (emphasis added)

10

Thus, the Examiner's objection against the specification is not justified.

This also applies to the written description requirement objection on page 5 of the Office Action. Examiner is of the opinion that this disclosure in the specification is sufficient for overcoming this objection.

15

Regarding detailed arguments with respect to the Saito reference, the Examiner is referred to Applicant's remarks in the response previously filed with the Patent Office.

20

The Examiner's rejection requires the Applicant to address the Downs reference. This reference does not disclose to leave the first part unencrypted. Instead, this reference discloses to completely encrypt a content. The idea to leave the first part unencrypted to provide a teaser and to make the header so that only a part of the header which is absolutely necessary for replaying the free first part of the user data so that the user can review the first part of the audio data without having to buy the full piece, is not at all disclosed in the Downs reference. Thus, this reference also does not disclose the features, which makes the invention new in view of Saito. To this end, please refer to column 3, lines 43 and 44.

25

30

The Rump reference, which corresponds to US patent 6,735,311 B1, which is assigned to the same assignee as in the present application, also discloses to encrypt the first part of an audio piece as illustrated in Fig. 3 and to leave the rest unencrypted, as also done in Fig. 4G of Saito. However, the idea to not encrypt the first part and to only encrypt the second part of the user payload data is also not at all disclosed in the Rump reference. In this context, note column 9, lines 16-19 of the US patent, which makes it clear that the free index, which the Examiner alludes to, does not have anything to do with deciphering, but only has to do with fully enabling a demo version of a deciphering device. In view of that, the Rump reference also does not disclose to leave the first part of user payload data unencrypted and to only encrypt the second part. All references of record only disclose at most, to encrypt the first part and to leave the second part unencrypted, which is completely contradictory to the present invention.

Should the Examiner find it helpful, he is encouraged to contact Applicant's attorney, Jeffrey Brill at (650) 474-8400.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Jeffrey Brill', with a stylized, flowing script.

Jeffrey Brill

Reg. No. 51,198

Customer No. 22,862

LISTING OF THE CLAIMS

1. (Currently Amended) A method for generating an encrypted user data
5 stream, which has a ~~start block~~header and a user data block, comprising
the following steps:

generating the ~~start block~~header; and

- 10 generating the user data block, which follows the ~~start block~~header, by
means of the following substeps:

using a first part of the user data as a start section for the user data
block, the start section remaining unencrypted;

15

encrypting a second part of user data which follow the first part of the
user data to obtain encrypted user data; and

appending the encrypted user data to the unencrypted start section.

20

2. (Currently Amended) A method according to claim 1, wherein the step of
generating the ~~start block~~header includes the following substep:

entering the length of the start section in the ~~start block~~header.

25

3. (Original) A method according to claim 1, wherein the second part does
not comprise all the user data to be encrypted and wherein the step of
generating the user data block includes the following substep:

30

appending a third part of user data to be encrypted, which follow the
second part, to the encrypted user data of the second part, the user data

of the third part being unencrypted.

4. (Currently Amended) A method according to claim 1, wherein the step of generating the ~~start block~~header includes the following substep:

5

entering the length of the encrypted user data of the second part which are encrypted, in the ~~start block~~header.

5. (Currently Amended) A method according to claim 3, wherein the step of generating the ~~start block~~header also includes the following substep:

10

entering the sum of the length of the encrypted user data, which correspond to the second part, and the length of the third part of the unencrypted user data in the ~~start block~~header.

15

6. (Currently Amended) A method for playing back an encrypted multimedia data stream, which has a ~~start block~~header and a user data block, where a start section of the user data block, which follows the ~~start block~~header, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the ~~start block~~header contains information which is needed to play back the start section of the user data block and where the ~~start block~~header contains information which is not needed to play back the unencrypted start section of the user data block, comprising the following steps:

20

25

processing the information of the ~~start block~~header which is needed to play back the start section of the user data block; and

playing back the unencrypted start section of the user data block.

30

7. (Currently Amended) A method according to claim 6, which also includes the following steps:

processing the information of the ~~start block~~header which is not needed to play back the unencrypted start section;

decrypting the further section of the user data block using the processed information of the ~~start block~~header; and

playing back the encrypted user data of the further section of the user data block.

8. (Currently Amended) A method according to claim 7, wherein the step of processing the information of the ~~start block~~header which is not needed to play back the unencrypted start section is performed concurrently with the playing back of the unencrypted start section.

9. (Original) A method according to claim 6, wherein the length of the unencrypted start section of the user data block is between 1 and 60 seconds.

10. (Original) A method according to claim 6, wherein the user data to be encrypted are coded and wherein the information which is needed for playing back contains an entry specifying the type of coding/decoding method.

11. (Original) A method according to claim 1, wherein the user data are audio and/or video data.

12. (Currently Amended) A device for generating an encrypted user data stream, which has a ~~start block~~header and a user data block, comprising:

a unit for generating the ~~start blockheader~~; and

a unit for generating the user data block, which follows the ~~start~~
5 ~~blockheader~~, with the following features:

a unit for using a first part of the user data as start section for the user
data block, the start section remaining unencrypted;

10 a unit for encrypting a second part of the user data which follows the
first part to obtain encrypted user data; and

a unit for appending the encrypted user data to the unencrypted start
section.

15

13. (Currently Amended) A device for playing back an encrypted user data
stream, which has a ~~start blockheader~~ and a user data block, where a
start section of the user data block, which follows the ~~start blockheader~~,
contains unencrypted user data and where a further section of the user
20 data block contains encrypted user data, where the ~~start blockheader~~
contains information which is needed to play back the start section of the
user data block and where the ~~start blockheader~~ contains information
which is not needed to play back the unencrypted start section of the user
data block, comprising:

25

a unit for processing only the information of the ~~start blockheader~~ which is
needed to play back the start section of the user data block; and

30

a unit for playing back the unencrypted start section of the user data block
in response to the unit for processing.

14. (Currently Amended) A device according to claim 13, which further comprises:

5 a unit for processing the information of the ~~start block~~header which is not needed to play back the unencrypted start section;

a unit for decrypting the further section of the user data block using the processed information of the ~~start block~~header; and

10 a unit for playing back the encrypted user data of the further section of the user data block.

15. (Currently Amended) A device according to claim 14, wherein the unit for processing the information of the ~~start block~~header which is not needed to play back the unencrypted start section is designed to be operated concurrently to the unit for playing back the unencrypted start section.

16. (Original) A device according to claim 13 which is implemented as a stereo system, hifi unit, solid state player, a playback unit with a hard disk or CD ROM, or a computer.

17. (Original) A device according to claim 12, wherein the user data are audio and/or video data.

- 25 18. (Currently Amended) A method of playing back an encrypted user data stream, which has a ~~start block~~header and a user data block, where a start section of the user data block, which follows the ~~start block~~header, contains unencrypted user data and where a further section of the user data block contains encrypted user data, where the ~~start block~~header contains information which is needed to play back the start section of the user data block and where the ~~start block~~header contains information
- 30

which is not needed to play back the unencrypted start section of the user data block, comprising:

5 processing only the information of the ~~start block~~header which is needed to play back the start section of the user data block; and

playing back the unencrypted start section of the user data block in response to the step of processing.

10

Fig.4A

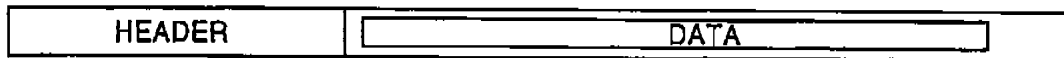


Fig.4B

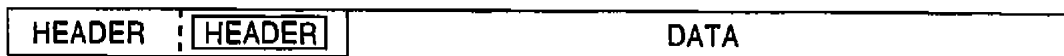


Fig.4C



Fig.4D



Fig.4E

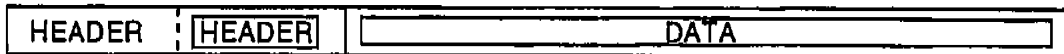


Fig.4F

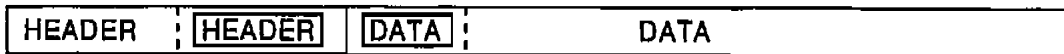
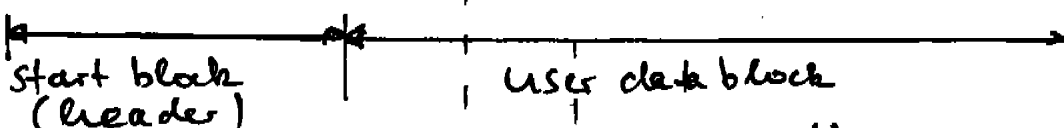


Fig.4G



(Prior Art)

Saito: start section is encrypted
2nd part is not encrypted

start section 2nd part

invention:
- start section: NOT encrypted
- 2nd part: encrypted